Delinea

El impacto de la alineación empresarial en la eficacia de la ciberseguridad

Encuesta mundial a responsables de ciberseguridad

DOCUMENTO TÉCNICO

Resumen ejecutivo

Hay formas obvias en que la ciberseguridad afecta a las empresas. Por ejemplo, cuando se produce un ciberataque a gran escala, el negocio puede detenerse repentinamente, como si un frenazo de emergencia hiciera descarrilar un tren que circula a toda velocidad.

Más allá de este escenario de descarrilamiento, el trabajo del equipo de ciberseguridad también repercute en la eficiencia empresarial diaria, la velocidad de prestación de servicios, los costes, la productividad de los empleados, la experiencia de los usuarios y las ventas. Aunque estos impactos no son tan dramáticos como la analogía del accidente de tren, pueden ralentizar el negocio y desviarlo de su curso de una forma que dificulta su recuperación.

La importancia de la alineación entre la ciberseguridad y la facilitación del negocio

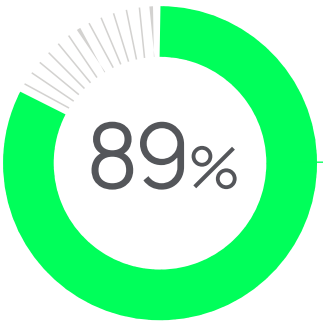
A medida que las organizaciones continúan navegando por un panorama informático complejo y un clima económico incierto, la alineación entre la ciberseguridad y la empresa es esencial para el éxito. Cada vez se dice más a los equipos de ciberseguridad que no deberían trabajar en silos, centrados únicamente en proteger la tecnología. Escuchan que no pueden ser el «departamento del no» y que en su lugar deben convertirse en «facilitadores del negocio».

Sin embargo, muchos no están seguros de cómo hacer realidad estas palabras de moda. La mayoría de los responsables de ciberseguridad tienen formación técnica y han ascendido en los departamentos técnicos. Es posible que hayan trabajado en un silo durante la mayor parte de su carrera. Cambiar de mentalidad para hacer posible una nueva forma de trabajar no se consigue de la noche a la mañana. El primer paso es llegar a una comprensión precisa y compartida de la situación actual del sector.

En este contexto, hemos encuestado a más de 2000 responsables de la toma de decisiones en materia de ciberseguridad en 22 países, que trabajan en empresas con más de 500 empleados, para comprender el estado actual de facilitación del negocio. Más concretamente, queríamos identificar con datos los tipos de atributos que tienen un impacto significativo en la facilitación del negocio, incluyendo la alineación, las habilidades y las estructuras organizativas.

Lo que hemos aprendido es fascinante y preocupante

Los resultados indican que al sector de la ciberseguridad le queda un largo camino por recorrer para convertirse en un facilitador del negocio eficaz. Los datos revelan una falta de alineación tanto entre los equipos como dentro de los equipos, lo que puede afectar negativamente a la postura de seguridad y a la consecución de los objetivos empresariales.



De hecho, el 89 % de los encuestados afirma que su empresa sufrió al menos un impacto negativo el año pasado debido a la falta de ciberseguridad y alineación empresarial.

Gran parte del problema radica en la incapacidad de las empresas para alinear eficazmente objetivos y métricas. Y gran parte de ese reto radica en la lucha de las organizaciones por alcanzar un acuerdo común en un amplio abanico de expectativas.

En este informe obtendrá una idea de la situación actual y conocerá algunos de los factores que determinan no solo la postura de ciberseguridad, sino también el éxito empresarial.

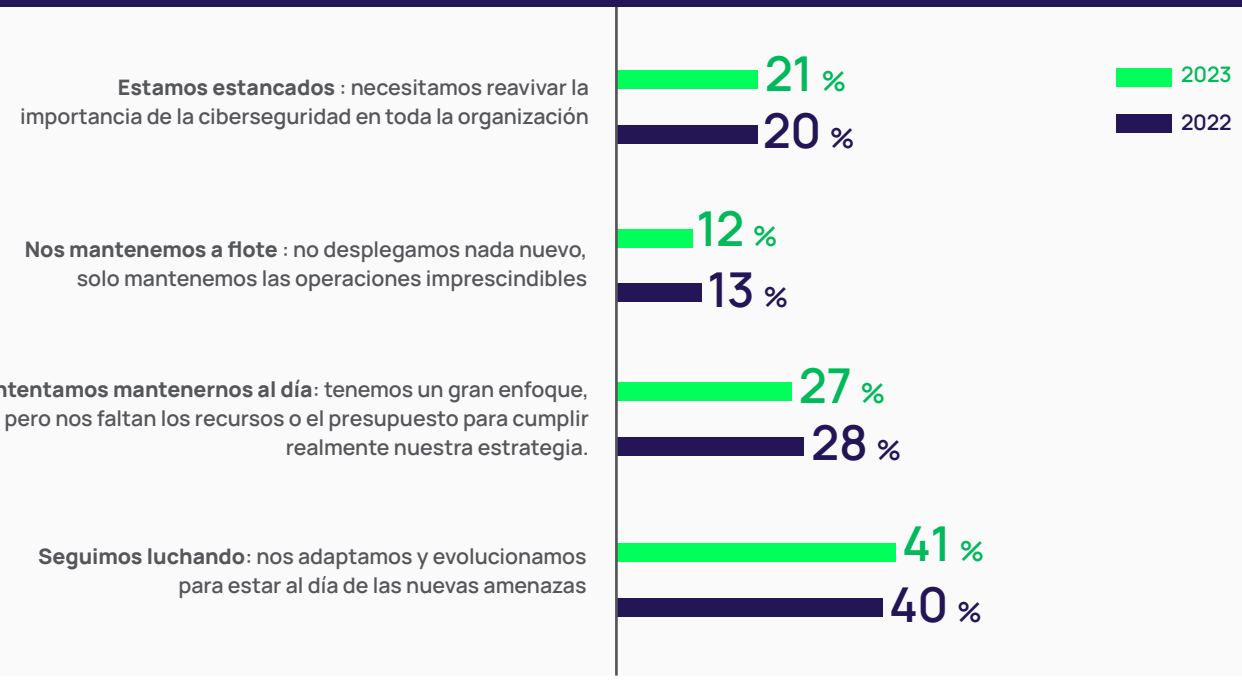
Conclusión principal 1

Cuando los responsables de ciberseguridad se sienten inseguros, es difícil centrarse en otra cosa

Aquí empezamos a entender el contexto en el que operan los responsables de la ciberseguridad.

Solo el 40 % de los encuestados afirman estar preparados para afrontar la lucha por la ciberseguridad. De hecho, la mayoría de los responsables de seguridad afirman que simplemente están rezagados, estancados o intentan mantenerse al día. Estos porcentajes prácticamente no han variado con respecto al año pasado.

Figura 1 | ¿Cuál de las siguientes opciones describe mejor su estrategia global de seguridad en este momento?



Curiosamente, los miembros de los equipos discrepan sobre el estado actual de la postura de seguridad de su empresa. Los que ocupan puestos de mayor responsabilidad se muestran más satisfechos con la situación actual de la seguridad que los que tienen responsabilidades cotidianas en materia de TI y gestión de la seguridad.

Figura 2 | ¿Cuál de las siguientes opciones describe mejor su estrategia global de seguridad en este momento?

	CEO	CISO/CIO/CSO	Director de TI o Seguridad	Responsable de TI o de Seguridad
Estamos estancados: necesitamos reavivar la importancia de la ciberseguridad en toda la organización	**39 %**	16 %	16 %	22 %
Nos mantenemos a flote: no desplegamos nada nuevo, solo mantenemos las operaciones imprescindibles	6 %	7 %	12 %	15 %
Intentamos mantenernos al día: tenemos un gran enfoque, pero nos faltan los recursos o el presupuesto para cumplir realmente nuestra estrategia	17 %	21 %	28 %	31 %
Seguimos luchando: nos adaptamos y evolucionamos para estar al día de las nuevas amenazas	38 %	**56 %**	**44 %**	**32 %**

Cambio de mentalidad

Cuando se considera la cuestión de la «facilitación del negocio» en este contexto, se ve por qué puede resultar difícil para un responsable de ciberseguridad ampliar sus competencias más allá de los aspectos básicos de seguridad. Muchos están inmersos en el esfuerzo diario por proteger la organización y combatir los peligros de forma reactiva cuando se producen. Por desgracia, esta falta de confianza en la seguridad significa que muchos responsables de ciberseguridad puede que no tengan la capacidad de centrarse también en los objetivos empresariales.

El verdadero problema de esta situación es el coste de oportunidad. La presión por alcanzar un nivel básico de seguridad «desplaza» la energía y los recursos necesarios para perseguir objetivos empresariales que tradicionalmente no son responsabilidad del equipo de seguridad.

Para un CISO que va a la zaga o intenta mantenerse al día, aconsejarle que se centre en los objetivos empresariales puede parecerle contrario a su visión del mundo. Pero, como veremos en este informe, cambiar el enfoque para incorporar objetivos empresariales puede tener también un impacto positivo en los objetivos de seguridad.

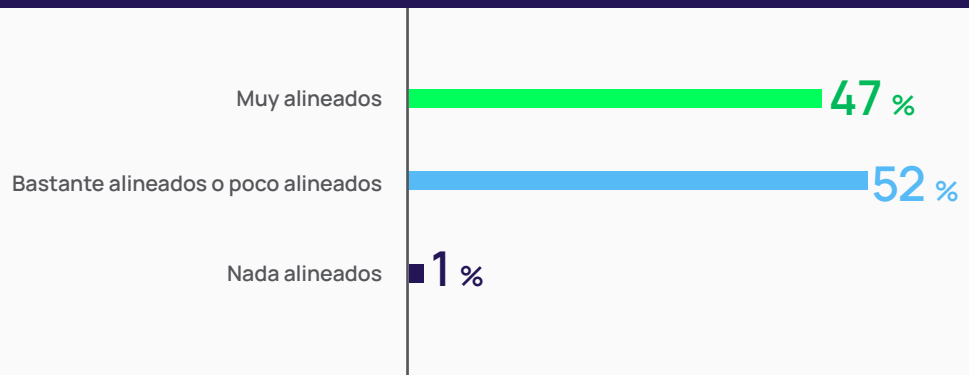
Conclusión principal 2

Los responsables de ciberseguridad reconocen que los objetivos empresariales son importantes, pero admiten que no los están cumpliendo

Los responsables en ciberseguridad admiten la falta de alineación entre los objetivos de seguridad y los empresariales

En general, menos de la mitad (47 %) de los directivos consideran que sus objetivos de ciberseguridad están muy alineados con los objetivos empresariales.

Figura 3 | ¿Cómo de alineados cree que están sus objetivos de ciberseguridad con los objetivos generales de la empresa?



Curiosamente, prácticamente todas las organizaciones que confían en su postura de seguridad –las que dicen que siguen luchando– ***también*** dicen estar muy o algo alineadas con los objetivos empresariales. En su caso, es mucho más probable que estén alineadas que las que dicen estar estancadas o intentan mantenerse al día de las necesidades de seguridad.

En el otro extremo del espectro, las organizaciones que menos confían en su postura de seguridad también creen que están alineados con los objetivos empresariales. Esto puede deberse a que o bien las empresas sobrestiman la alineación entre seguridad y negocio, o bien subestiman su postura en materia de ciberseguridad.

Figura 4 | ¿Cómo de alineados cree que están sus objetivos de ciberseguridad con los objetivos generales de la empresa?

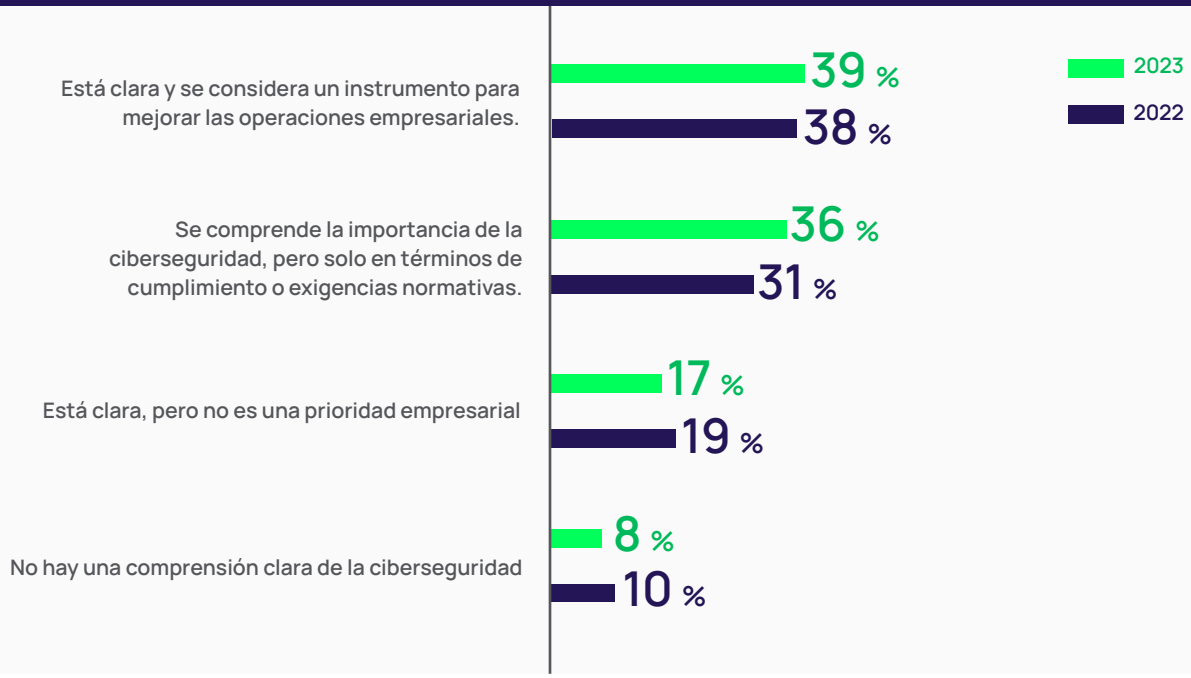
	Muy alineados	Bastante alineados	Poco alineados	Nada alineados	No estoy seguro
Estamos estancados: necesitamos reavivar la importancia de la ciberseguridad en toda la organización	59 %	36 %	4 %	1 %	1 %
Nos mantenemos a flote: no desplegamos nada nuevo, solo mantenemos las operaciones imprescindibles	29 %	56 %	13 %	2 %	0 %
Intentamos mantenernos al día: tenemos un gran enfoque, pero nos faltan los recursos o el presupuesto para cumplir realmente nuestra estrategia	31 %	60 %	7 %	2 %	0 %
Seguimos luchando: nos adaptamos y evolucionamos para estar al día de las nuevas amenazas	56 %	43 %	1 %	0 %	0 %

Los niveles más altos de una organización no comprenden la conexión entre empresa y seguridad

La función de la ciberseguridad aún no es reconocida como un elemento facilitador del negocio por los niveles más altos de la organización. Aunque la mitad de los encuestados (53 %) afirma que su consejo de administración y dirección ejecutiva entienden la función la ciberseguridad, creen que estos directivos no la ven como un elemento facilitador del negocio. Esta cifra no ha variado mucho en el último año.

Es una historia dolorosa, pero indicativa de lo desalineados que están los objetivos de ciberseguridad y de negocio dentro de la empresa.

Figura 5 | ¿Cuál de las siguientes afirmaciones describe mejor la comprensión de la ciberseguridad por parte del Consejo de Administración/los directivos de su organización?

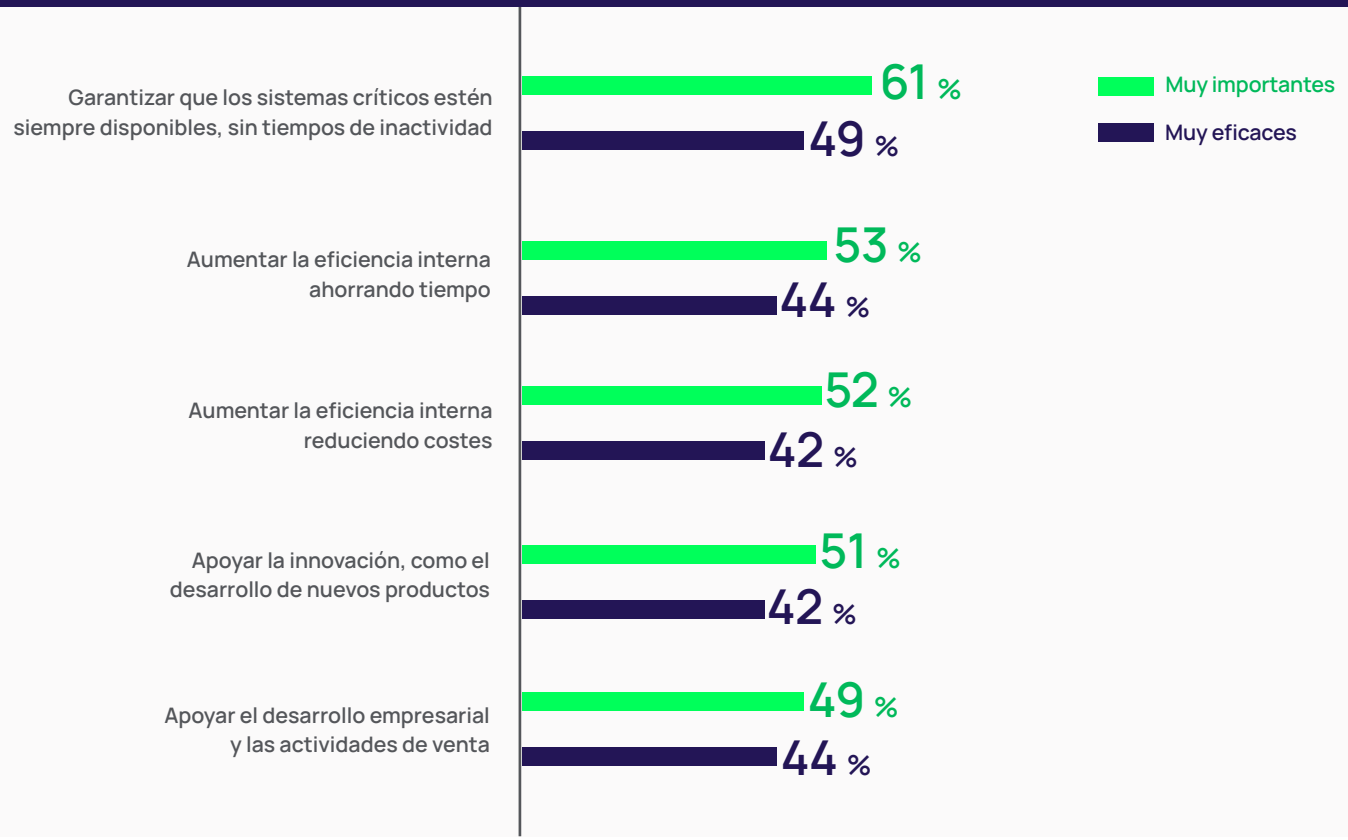


Los responsables de ciberseguridad no creen ser eficaces a la hora de alcanzar sus máximas prioridades

Resulta que, aunque el objetivo principal de la mayoría de los responsables de la seguridad es de carácter ***técnico*** —garantizar la protección y disponibilidad de los sistemas críticos—, aproximadamente la mitad también cree que los objetivos ***empresariales***, como aumentar la eficiencia, reducir los costes, apoyar la innovación y respaldar las ventas, también son importantes para que sus equipos los alcancen.

Sin embargo, menos de la mitad cree ser muy eficaz a la hora de alcanzar sus objetivos prioritarios, tanto los objetivos técnicos como los empresariales.

Figura 6 | ¿Qué importancia tienen los siguientes objetivos para su equipo de ciberseguridad? ¿Cuál cree que es la eficacia de su equipo de ciberseguridad para alcanzar esos objetivos?



Del mismo modo, las empresas que confían más en su postura de seguridad tienen más probabilidades de ser muy ***eficaces*** a la hora de cumplir los objetivos empresariales. Una vez más, los equipos de seguridad menos confiados afirman que son eficaces, como muestra el gráfico siguiente.

Figura 7 | ¿Cuál cree que es la eficacia de su equipo de ciberseguridad para alcanzar esos objetivos?

	Garantizar que los sistemas críticos estén siempre disponibles, sin tiempos de inactividad	Apoyar el desarrollo empresarial y las actividades de venta	Aumentar la eficiencia interna ahorrando tiempo	Apoyar la innovación, como el desarrollo de nuevos productos	Aumentar la eficiencia interna reduciendo costes
Estamos estancados: necesitamos reavivar la importancia de la ciberseguridad en toda la organización	62 %	60 %	65 %	58 %	61 %
Nos mantenemos a flote: no desplegamos nada nuevo, solo mantenemos las operaciones imprescindibles	51 %	49 %	44 %	40 %	43 %
Intentamos mantenernos al día: tenemos un gran enfoque, pero nos faltan los recursos o el presupuesto para cumplir realmente nuestra estrategia	53 %	48 %	42 %	40 %	48 %
Seguimos luchando: nos adaptamos y evolucionamos para estar al día de las nuevas amenazas	62 %	53 %	55 %	55 %	48 %

Cambio de mentalidad

Esta falta de alineación puede deberse a varias razones. Algunas de ellas podrían ser:

1. **Falta de alineación entre los objetivos de seguridad y los empresariales:** es posible que los responsables de seguridad se centren demasiado en mitigar los riesgos y proteger los activos sin comprender los objetivos empresariales más amplios.

2. **Falta de comunicación y colaboración:** es posible que los responsables de seguridad no comuniquen eficazmente sus metas y objetivos a otras unidades de negocio o partes interesadas, o que no colaboren con ellas para desarrollar estrategias de seguridad que respalden los objetivos empresariales. Esto puede dar lugar a que las medidas de seguridad se consideren impedimentos para los objetivos empresariales en lugar de facilitadores.

3. **Recursos insuficientes:** es posible que los responsables de seguridad no dispongan de recursos suficientes, como presupuesto, personal o tecnología, para implementar medidas de seguridad que cumplan los objetivos de la empresa. Esto puede dar lugar a que las medidas de seguridad sean inadecuadas o ineficaces, o que impongan cargas a otras unidades de negocio.

4. **Métricas inadecuadas:** es posible que los responsables de seguridad no dispongan de las métricas adecuadas para cuantificar la eficacia de sus medidas a la hora de cumplir los objetivos empresariales. Esto puede dar lugar a que las medidas de seguridad se perciban como ineficaces, aunque lo sean.

5. **Falta de comprensión de los objetivos empresariales:** es posible que los responsables de seguridad no comprendan claramente los objetivos, prioridades y retos empresariales de la organización. Esto puede dar lugar a que las medidas de seguridad no tengan en cuenta las necesidades específicas de la empresa.

Profundizaremos en cada una de estas posibles razones a lo largo del resto del informe.

Conclusión principal 3

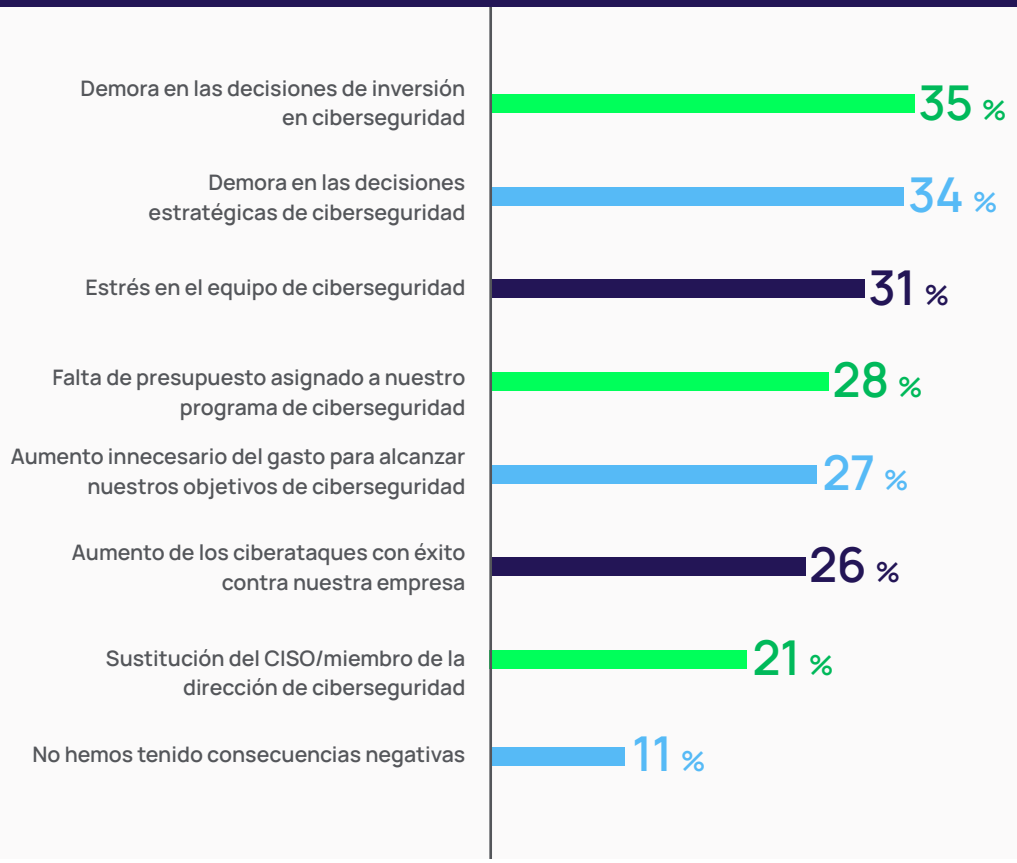
La falta de alineación tiene un impacto negativo **tanto** en los objetivos empresariales **como** de seguridad

Un ciberataque con éxito puede dar lugar a filtraciones de datos, paradas del sistema, pérdidas económicas y daños a la reputación de una empresa, todo lo cual puede socavar sus objetivos de negocio. Los resultados del estudio respaldan esta afirmación.

Los efectos negativos son muy variados

Cerca de nueve de cada diez organizaciones ha sufrido al menos una consecuencia negativa el año pasado debido a la falta de ciberseguridad y alineación empresarial.

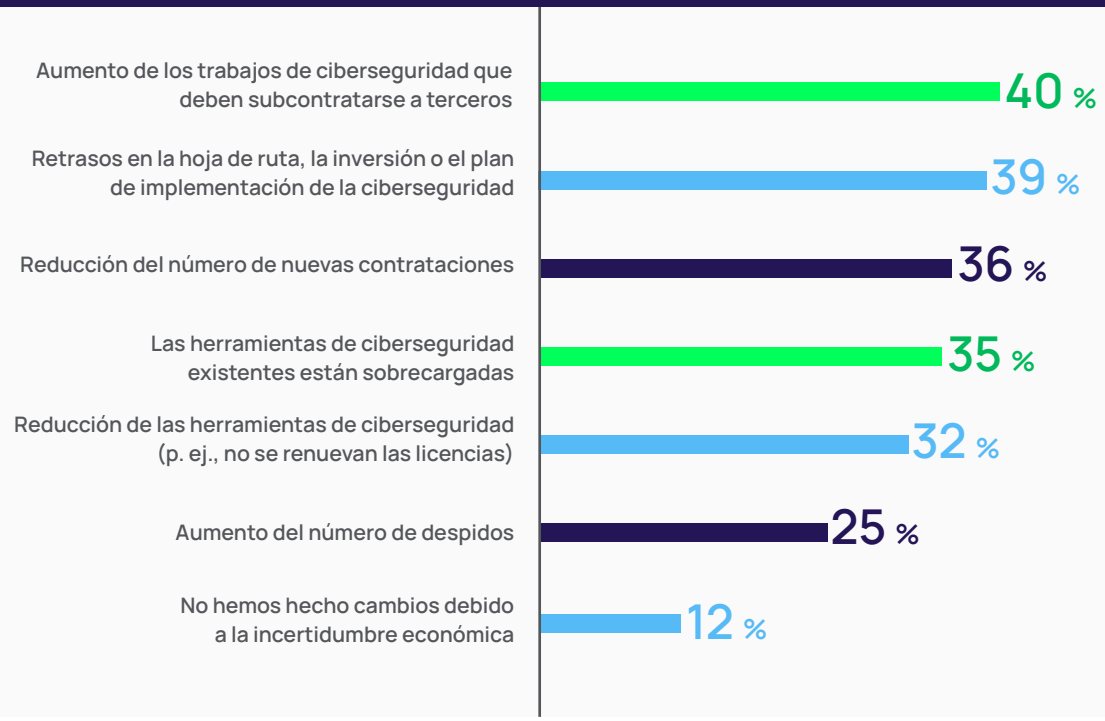
Figura 8 | ¿Qué consecuencias negativas, en su caso, ha experimentado debido a la falta de alineación de los objetivos de ciberseguridad y empresariales? (Seleccione hasta tres).



¿Por qué ahora? El clima económico actual tiene parte de culpa

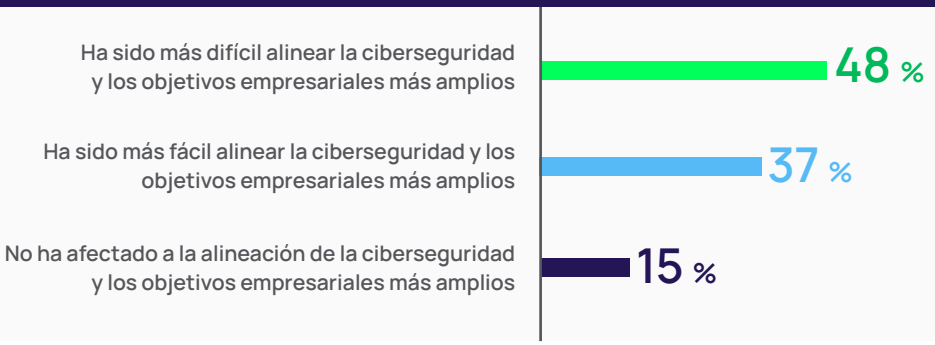
El 88 % ha experimentado cambios debido a la incertidumbre económica. Muchos de estos cambios repercuten negativamente en la seguridad, como la ralentización de la hoja de ruta y la inversión en tecnología, así como la falta de recursos, tal y como muestra el siguiente gráfico.

Figura 9 | ¿Cómo ha afectado la reciente incertidumbre económica a su equipo de ciberseguridad en los últimos 6 meses?



En un entorno de cambio, la alineación puede suponer un reto. Aproximadamente la mitad de los encuestados está de acuerdo en que la incertidumbre económica ha hecho que la ciberseguridad y la alineación empresarial sean más difíciles de conseguir.

Figura 10 | ¿Cómo ha afectado la reciente incertidumbre económica a la alineación de los objetivos de ciberseguridad y los objetivos empresariales más amplios?



Cambio de mentalidad

Con desafíos como estos, la verdadera pregunta sobre la seguridad y la alineación empresarial no es «¿Cómo podemos permitirnos hacerlo?», sino «¿Cómo podemos permitirnos no hacerlo?».

Al incorporar la ciberseguridad como parte de la estrategia empresarial global de una empresa, se puede desarrollar un enfoque proactivo de la seguridad que permite reducir el riesgo de ciberataques y ayudar a salvaguardar las operaciones empresariales críticas.

Recurso clave:

Global Survey of Cybersecurity Leaders: Benchmarking Security Gaps & Privileged Access

Conclusión principal 4

La falta de alineación entre la ciberseguridad y la empresa se refleja en unas métricas desajustadas.

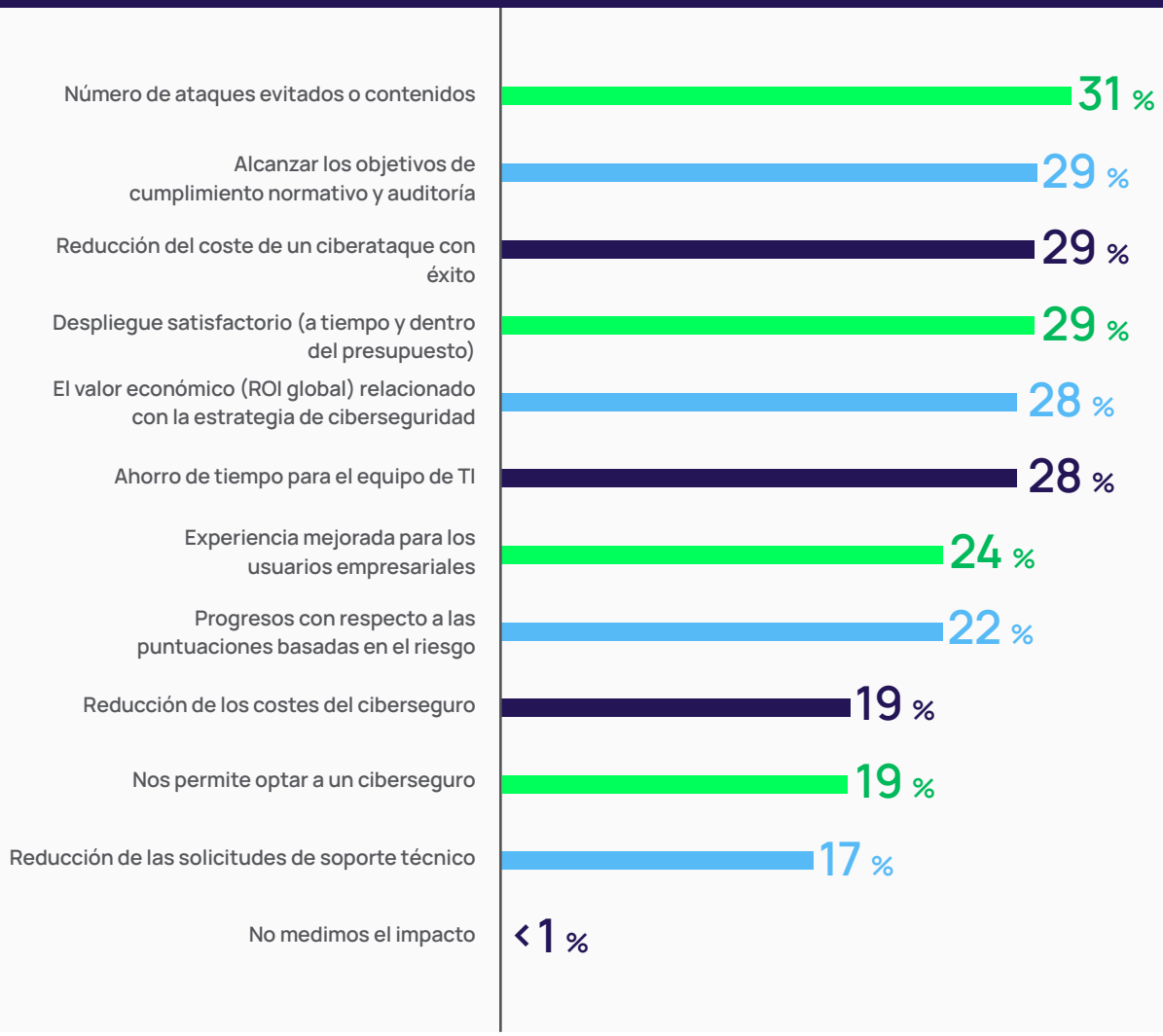
Como dice el dicho, si quieres mejorar algo, tienes que medirlo. Para alcanzar las metas de facilitación del negocio, los objetivos de equipo y los OBM individuales (Gestión por Objetivos) u OKR (Objetivos y Resultados Clave) deben estar vinculados y ser objeto de un seguimiento continuo.

Por desgracia, salvo algunas excepciones, no parece ser así. No es lo mismo lo que los directivos quieren hacer que lo que realmente miden y comunican.

Diferencia entre métricas técnicas y empresariales

Los datos muestran que el rendimiento de los programas de ciberseguridad se sigue juzgando principalmente en función de métricas técnicas o basadas en actividades, como el número de ataques evitados o contenidos, en lugar de métricas orientadas al negocio, como el valor económico, la experiencia del usuario, los costes de los seguros o el impacto en otros equipos.

Figura 11 | ¿Cuál de los siguientes aspectos es el más importante a la hora de medir el éxito de sus programas de ciberseguridad? (Seleccione hasta tres).



Dicho esto, el retorno de la inversión/valor económico global es más importante para las empresas más pequeñas con menos empleados.

Figura 12 | ¿Cuál de los siguientes aspectos es el más importante a la hora de medir el éxito de sus programas de ciberseguridad? (Seleccione hasta tres).

	1.º	2.º	3.º
500-999 empleados	El valor económico (ROI global, **29 %**)	Número de ataques evitados/Reducción de costes/Ahorro de tiempo (todos **28 %**)	
1000-4999 empleados	Número de ataques evitados/ contenidos (**32 %**)	Despliegue satisfactorio/Ahorro de tiempo para el equipo de TI (ambos **31 %**)	
+5000 empleados	Número de ataques evitados o contenidos/Cumplir los objetivos de cumplimiento normativo y auditorías (ambos **31 %**)		Reducción del coste de ciberataques con éxito (**30 %**)

No es de extrañar que los directivos con una amplia responsabilidad organizativa, como los CEO/propietarios, estén más preocupados que los CISO por medir la experiencia del usuario y reducir la fricción. Sin embargo, es interesante observar que los niveles directivos/responsables de departamento también hacen hincapié en métricas empresariales como el valor económico/ROI.

Figura 13 | ¿Cuál de los siguientes aspectos es el más importante a la hora de medir el éxito de sus programas de ciberseguridad? (Seleccione hasta tres).

	1.º	2.º	3.º
CEO/ Propietario de la empresa	Experiencia mejorada para los usuarios empresariales (**31 %**)	Implementación satisfactoria (a tiempo, dentro del presupuesto, **30 %**)	Cumplir los objetivos de cumplimiento normativo y auditoría (**29 %**)
CIO/CSO /CISO	Número de ataques evitados/ contenidos (**32 %**)	Despliegue satisfactorio (a tiempo y dentro del presupuesto, **31 %**)	El valor económico/Reducción del coste/Cumplimiento de los objetivos (todos **28 %**)
Jefe del Departamento de TI	El valor económico (ROI global, **34 %**)	Número de ataques evitados/ contenidos (**32 %**)	Reducción de costes/Cumplimiento de los objetivos (ambos **30 %**)
Director de TI	El valor económico (ROI global, **32 %**)	Número de ataques evitados o contenidos/Ahorro de tiempo para el equipo de TI (ambos **30 %**)	
Responsable de TI	Número de ataques evitados/ contenidos (**33 %**)	Reducción del coste/Cumplimiento de los objetivos/Despliegue satisfactorio (todos **30 %**)	
Responsable de seguridad	Reducción del coste de ciberataques con éxito (**36 %**)	Despliegue satisfactorio (a tiempo y dentro del presupuesto, **29 %**)	Alcanzar los objetivos de cumplimiento normativo y auditoría (**27 %**)

Cambio de mentalidad

Los equipos de ciberseguridad suelen centrarse en las métricas técnicas, porque proporcionan datos que pueden utilizarse para evaluar la postura de seguridad de una organización. Las métricas técnicas, como el número de vulnerabilidades detectadas y parcheadas, el tiempo que se tarda en detectar y responder a incidentes de seguridad, y el porcentaje de sistemas con software de seguridad actualizado, proporcionan información sobre la eficacia de los controles de seguridad y permiten a los equipos identificar áreas de mejora.

Sin embargo, aunque las métricas técnicas son importantes, no son los únicos factores que determinan el éxito de un programa de ciberseguridad. En última instancia, la ciberseguridad está al servicio de los objetivos empresariales: resultados estratégicos que son posibles gracias a una seguridad eficaz.

Los responsables de ciberseguridad pueden mejorar la alineación estableciendo objetivos empresariales claros y medibles que estén vinculados a los objetivos estratégicos de su organización. Esto podría implicar la identificación de los activos más críticos para la empresa, el impacto potencial para el negocio empresa si esos activos fueran atacados y en qué medida unos controles de seguridad eficaces mejoran la disponibilidad, confidencialidad e integridad de esos activos. Por ejemplo, cuando el servicio no funciona, el coste económico y operativo es evidente. Los resultados de la ciberseguridad pueden medirse por el coste de no hacer nada frente al coste de hacer algo.

Los equipos de ciberseguridad también podrían trabajar para mejorar su comunicación y colaboración con otras partes de la organización, como la gestión de riesgos, el cumplimiento y las operaciones empresariales. Trabajando en estrecha colaboración con estas partes interesadas, los equipos de ciberseguridad pueden comprender mejor el contexto y las prioridades de la empresa, y alinear sus actividades en consecuencia.

Por último, los equipos de ciberseguridad podrían considerar la adopción de un enfoque de la seguridad más basado en los riesgos, en el que las métricas técnicas se utilicen junto con los resultados empresariales para fundamentar la toma de decisiones. Esto implicaría identificar los riesgos más significativos para la empresa y, a partir de ahí, centrar los recursos en mitigar esos riesgos en lugar de limitarse a aplicar métricas técnicas sin más.

Para medir la ciberseguridad en función de los objetivos empresariales, tenga en cuenta lo siguiente:

1. **Responsables de la gestión de riesgos:** para medir la eficacia de una empresa a la hora de identificar y mitigar los riesgos de ciberseguridad, incluida la frecuencia de los incidentes y los tiempos de respuesta.

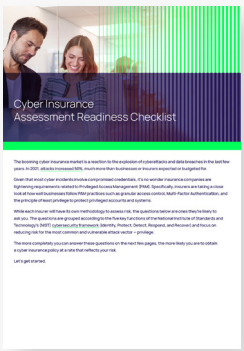
2. **Métricas de cumplimiento:** para saber hasta qué punto una empresa cumple las normas reglamentarias y del sector en materia de ciberseguridad.

3. **Métricas de continuidad del negocio:** para medir la capacidad de una empresa para mantener las operaciones comerciales durante un incidente de ciberseguridad, incluida la duración del tiempo de inactividad y el tiempo de recuperación.

4. **Métricas de costes:** para realizar un seguimiento del coste de despliegue y mantenimiento de las medidas de ciberseguridad en relación con el presupuesto global.

5. **Métricas de productividad:** para medir la rapidez con la que se puede incorporar a un nuevo empleado o proveedor y proporcionarle los recursos y el acceso necesarios para realizar su trabajo.

Mediante el uso de este tipo de métricas, puede evaluar la eficacia de su estrategia de ciberseguridad permitiendo a la organización alcanzar los objetivos empresariales y tomar decisiones informadas sobre las inversiones en recursos de ciberseguridad.



Recursos clave:

- Cyber Insurance Readiness Checklist: responda a las preguntas que seguramente le harán los proveedores de ciberseguros
- Alinearse a los marcos normativos y a los requisitos de cumplimiento normativo

Conclusión principal 5

Sin cambios estructurales, las señales apuntan a un camino difícil para la ciberseguridad y la alineación empresarial

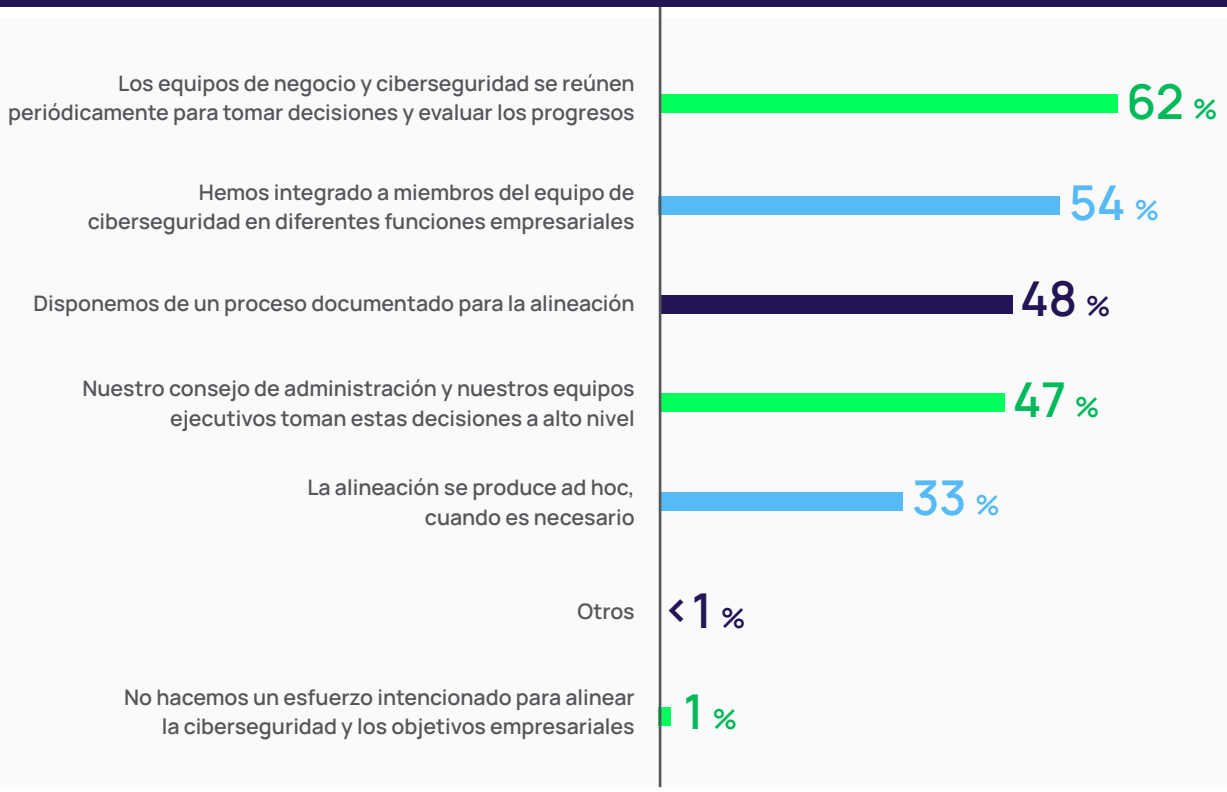
Para que la empresa y la ciberseguridad estén alineadas, es esencial tener en cuenta la estructura organizativa. Este es el aspecto que trataremos a continuación.

Hablar y actuar

La buena noticia es que se están produciendo conversaciones interfuncionales en la empresa. La mayoría de los equipos de ciberseguridad se reúnen regularmente con sus homólogos de la empresa en los niveles altos o incluso tienen miembros del equipo de seguridad integrados en las funciones empresariales.

Sin embargo, menos de la mitad de las organizaciones están documentando políticas y procedimientos para ayudarles a alinearse.

Figura 14 | ¿Cómo se asegura tu organización de que los objetivos de ciberseguridad están alineados con los objetivos empresariales más amplios? (Seleccione todo lo que proceda).



Los encuestados que se califican a sí mismos como **«muy alineados»** son los más propensos a decir que:

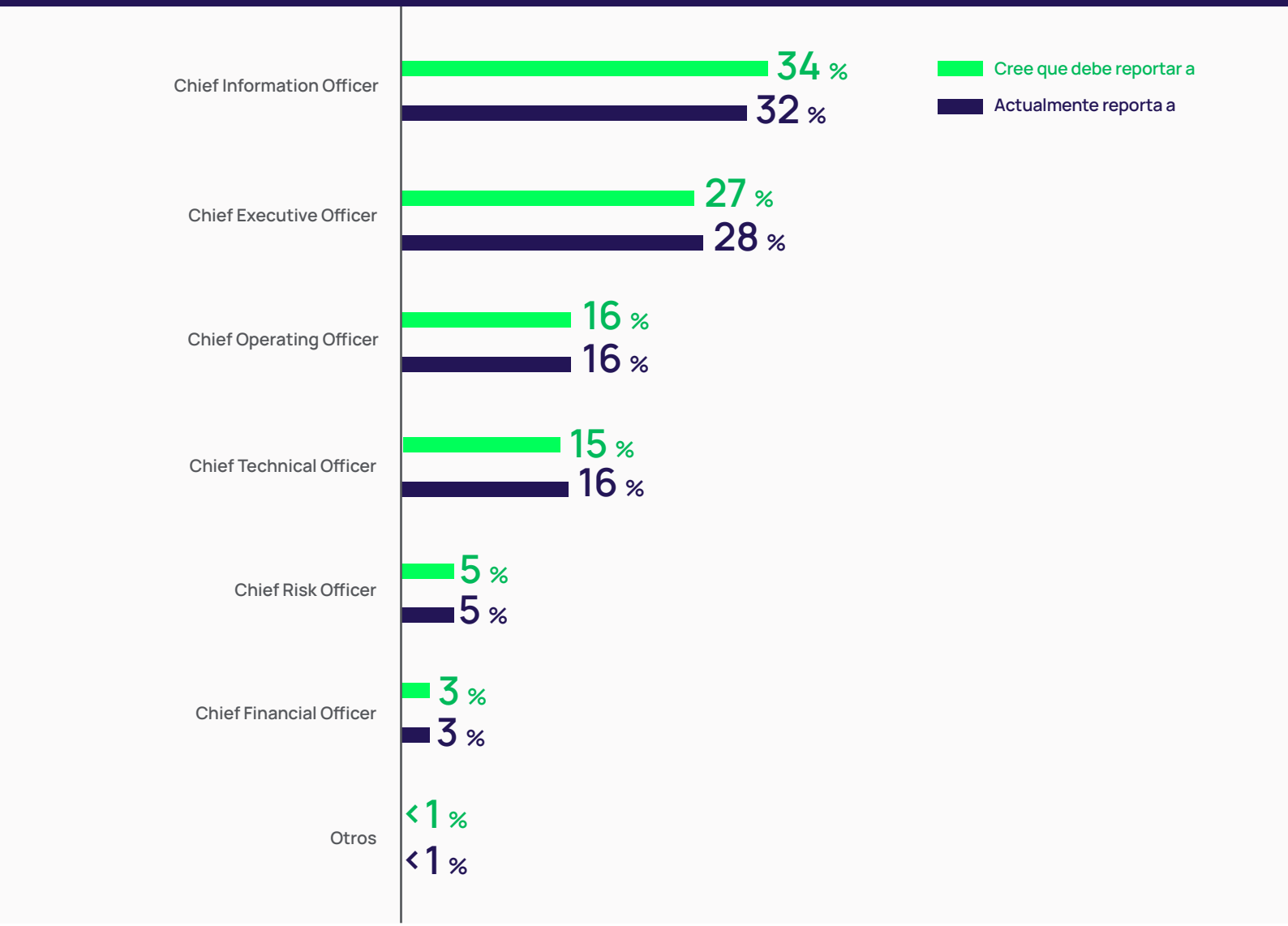
- Los equipos de negocio y ciberseguridad se reúnen regularmente para tomar decisiones y evaluar el progreso (68 %)
- Hemos integrado a miembros del equipo de ciberseguridad en diferentes funciones empresariales (61 %)
- Nuestro consejo de administración y equipos ejecutivos toman estas decisiones a alto nivel (56 %)

La estructura de informes puede perjudicar más que ayudar a la facilitación del negocio

Más de un tercio (34 %) de los encuestados cree que la persona adecuada a la que debe reportar un CISO es el CIO. Y, de hecho, en la mayoría de las organizaciones, es a él a quien rinden cuentas.

Es interesante observar que las preferencias de información varían en función del cargo. Por ejemplo, es más probable que los CEO prefieran que los CISO dependan de ellos, mientras que los directores de TI son más propensos a decir que los CISO deberían depender de su jefe, el CIO.

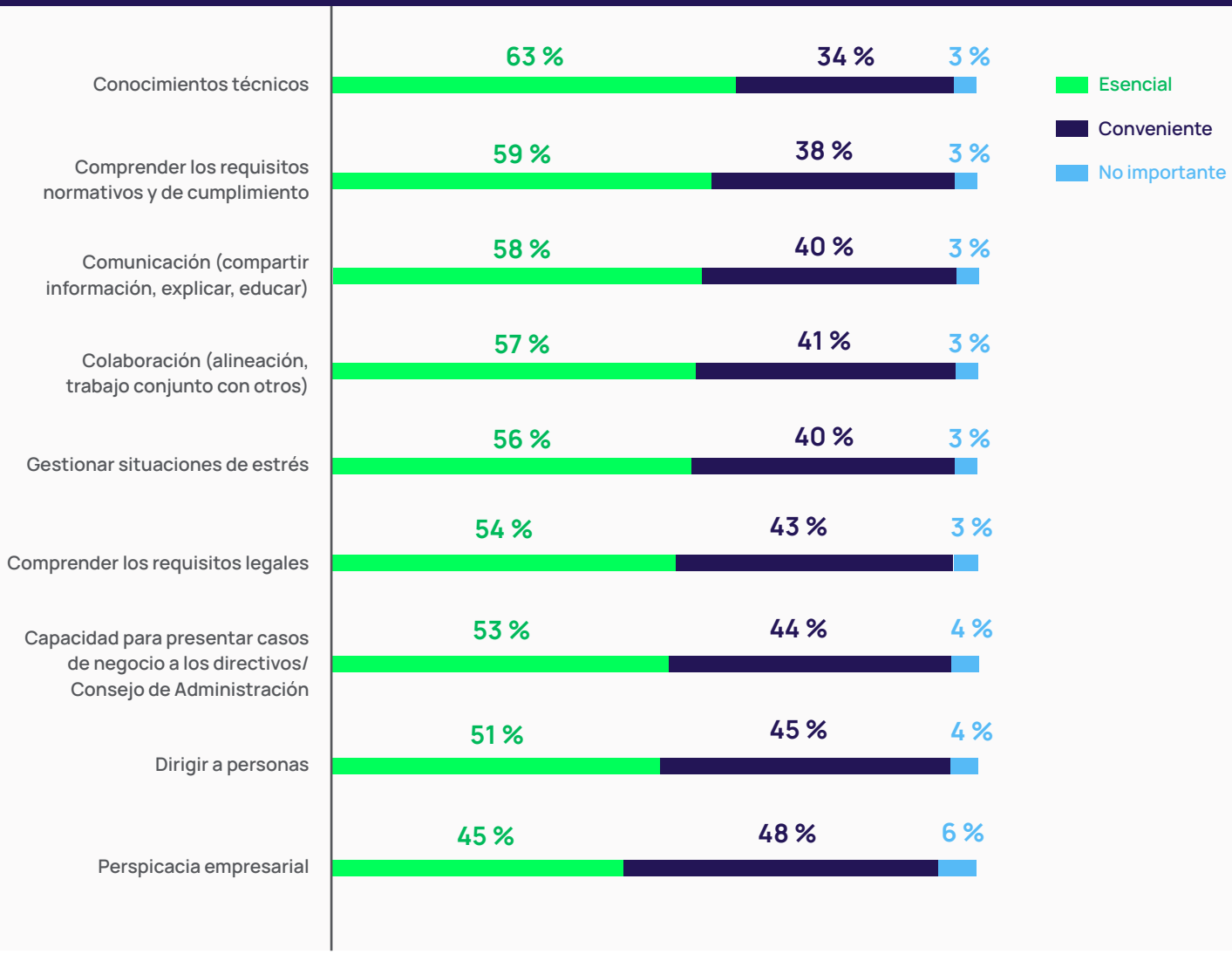
Figura 15 | ¿De quién cree que debería depender el CISO o el responsable de ciberseguridad de mayor rango para alinear mejor la ciberseguridad con los objetivos generales de la empresa? En la actualidad, ¿a quién reporta el CISO o el responsable de ciberseguridad de mayor rango en tu organización?



Las habilidades actuales reflejan la necesidad de un mayor enfoque empresarial entre los responsables de ciberseguridad

En general, los encuestados creen que los conocimientos técnicos son la habilidad esencial para un responsable de ciberseguridad como un CISO. Consideran esta habilidad mucho más importante que otras relacionadas con la empresa, como la comunicación, la colaboración, la presentación de un caso de negocio y la perspicacia empresarial.

Figura 16 | ¿En qué medida son importantes cada una de estas habilidades para un CISO/responsable de ciberseguridad? Selecciona una por fila



Como se ve en el gráfico siguiente, las habilidades que los encuestados creen sus principales carencias son la capacidad de dirigir o reducir situaciones de estrés, seguidas de la presentación de casos de negocio y la comunicación. Sin estas habilidades, los responsables de ciberseguridad tendrán muchas dificultades para alinearse con sus homólogos en la empresa.

Figura 17 | ¿Cuáles cree que son sus propias carencias? Seleccione todo lo que proceda

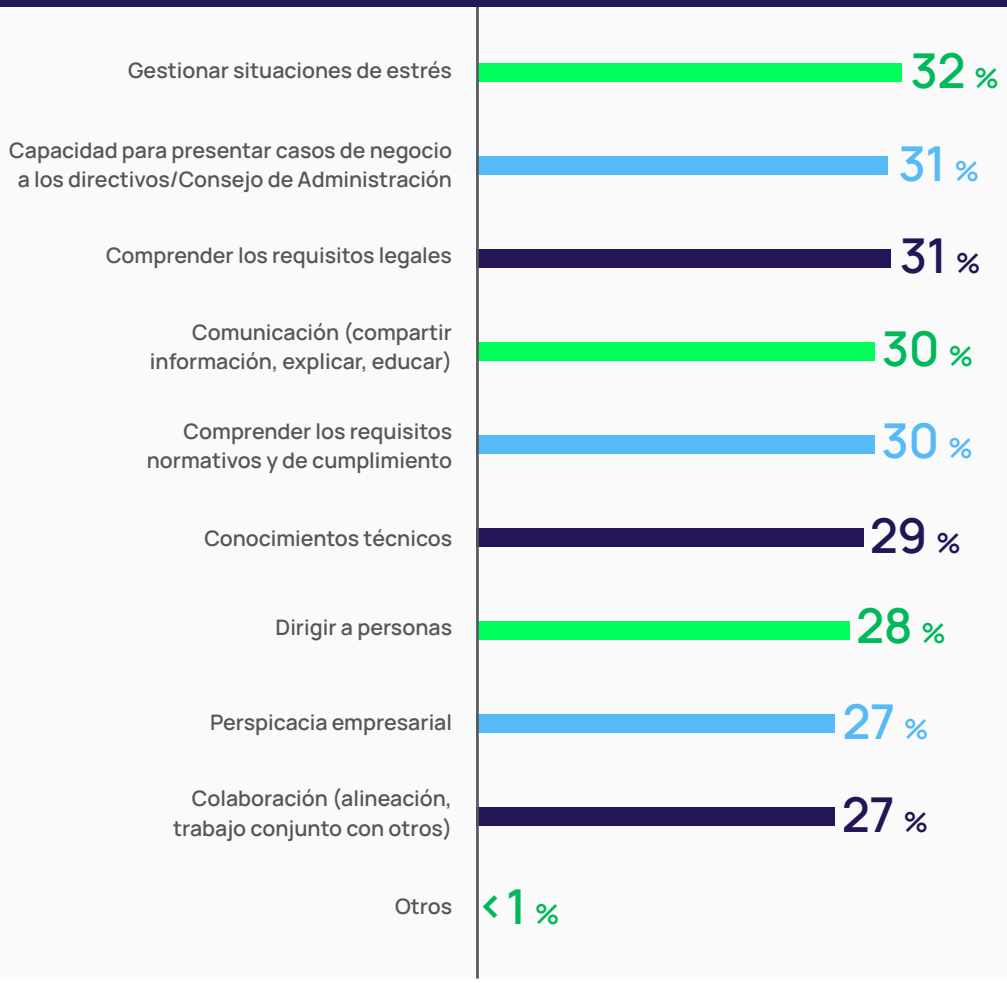


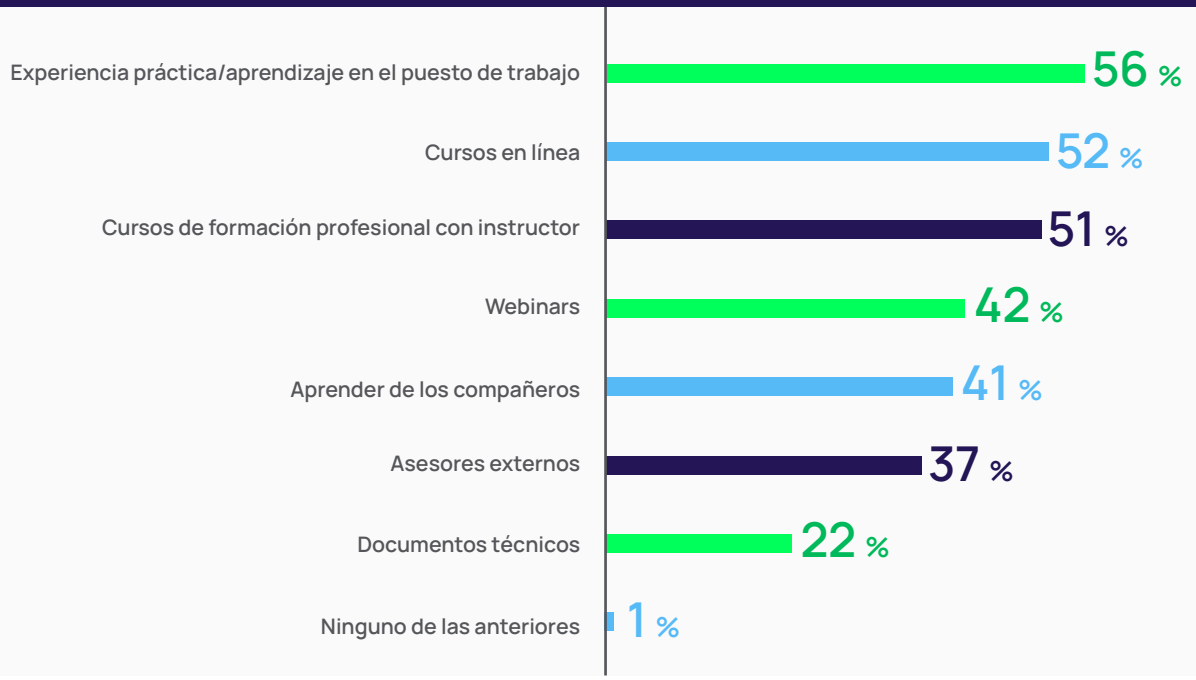
Figura 18 | ¿Cuáles crees que son tus propias carencias?

	1.º	2.º	3.º
CEO/Propietario de la empresa	Gestionar situaciones de estrés/Comunicación (compartir información, explicar, educar, ambos **38 %**)		Capacidad para presentar casos de negocio a los directivos/Consejo de Administración (**36 %**)
CIO/CSO/ CISO	Comprender los requisitos legales/Conocimientos técnicos (**32 %**)	Gestionar situaciones de estrés/Capacidad para presentar casos de negocio a los directivos/Comunicación/Comprender los requisitos normativos y de cumplimiento (todos **31 %**)	
Jefe del Departamento de TI	Gestionar situaciones de estrés (**31 %**)	Comprender los requisitos legales/Comunicación/Dirigir a personas (todos **29 %**)	
Director de TI	Gestionar situaciones de estrés (**32 %**)	Comprender los requisitos legales (**31 %**)	Comprender los requisitos normativos y de cumplimiento (**30 %**)
Responsable de TI	Capacidad para presentar casos de negocio a los directivos/ Consejo de Administración (**34 %**)	Reducción del coste/Cumplimiento de los objetivos/Despliegue satisfactorio (todos **30 %**)	
Responsable de seguridad	Dirigir a personas (**37 %**)	Perspicacia empresarial (**29 %**)	Capacidad para presentar con éxito argumentos comerciales a la alta dirección y Consejos de Administración/ Colaboración (ambos **28 %**)

La formación reactiva no suple la falta de habilidades

La experiencia práctica y el aprendizaje en el puesto de trabajo son las formas más habituales que tienen los encuestados de mejorar sus habilidades. Parece que la actitud general es «ya nos ocuparemos de ese problema cuando tengamos que hacerlo». Esto no es un buen augurio para el desarrollo de las habilidades necesarias para una facilitación del negocio proactiva e intencionada.

Figura 19 | ¿ Cómo mejoras tus propias habilidades y te formas para alinearte con los objetivos empresariales y mejorar el rendimiento general de la empresa?



Dicho esto, como ya debería haber quedado claro, la capacitación empresarial no es solo un reto de «habilidades». También puede ser un desafío a la «voluntad».

Cambio de mentalidad

Para alinearse mejor y cumplir el objetivo de «facilitación del negocio», los responsables de ciberseguridad deben tener en cuenta lo siguiente:

Celebrar reuniones efectivas

Naturalmente, se podría pensar que la mejor manera de impulsar la alineación es, en primer lugar, reunir a todos. Pero reunirse a menudo no garantiza la alineación. De hecho, ese tipo de reunión podría no ser necesaria en absoluto. La alineación consiste en conseguir que los equipos interactúen entre sí de una manera muy concreta, independientemente de que se reúnan o no.

Al fin y al cabo, la alineación puede ser sincrónica o asincrónica. En un mismo lugar o distribuidos. En persona o a través de una llamada Zoom. Siempre que ayude a los equipos a entenderse, compartir objetivos y medir colectivamente el éxito.

Desarrollo de habilidades

Es bastante probable que las organizaciones no encuentren en una sola persona la combinación perfecta de competencias de seguridad y empresariales. Para encontrar la combinación adecuada, los responsables de ciberseguridad tendrán que mirar más allá de los expertos técnicos e incorporar a personas con formación no tradicional para que trabajen con sus equipos.

Reconsiderar la estructura jerárquica

Si bien el hecho de que el CISO reporte al CIO puede tener sus ventajas, también puede plantear problemas.

¿Debe el CISO depender del CIO?

INCONVENIENTES

- **Alineación con la estrategia de TI:** el CISO y el CIO colaboran estrechamente para alinear la estrategia de seguridad de TI de la organización con su estrategia empresarial global. Este planteamiento garantiza la integración de la seguridad en todos los aspectos de TI, incluido el desarrollo y la implementación de nuevas tecnologías, aplicaciones e infraestructuras.

- **Responsabilidad clara:** al depender del CIO, el CISO es claramente responsable de la seguridad de los sistemas de TI de la organización. Esta responsabilidad contribuye a garantizar que los riesgos de seguridad se identifiquen, evalúen y aborden con prontitud y eficacia.

- **Asignación de recursos:** el CIO es responsable de asignar recursos a los proyectos de TI, y al tener al CISO bajo su responsabilidad, se garantiza que la seguridad se tenga en cuenta en la asignación de recursos. El CISO puede ayudar al CIO a identificar las áreas en las que se necesitan recursos adicionales para reforzar la postura de seguridad de la organización.

- **Mejor comunicación:** el CISO y el CIO comprenden mejor los retos a los que se enfrentan mutuamente y pueden trabajar juntos para abordarlos. Al depender del CIO, el CISO tiene mejor acceso a los responsables de la toma de decisiones de TI y puede comunicarse más eficazmente con ellos.

VENTAJAS

- **Conflicto de intereses:** el CIO es responsable de prestar servicios y proyectos de TI a tiempo y dentro del presupuesto. Este enfoque en la entrega a veces puede entrar en conflicto con la responsabilidad del CISO de garantizar la seguridad de los sistemas informáticos. Este conflicto puede llevar a que el CISO se vea presionado para dar prioridad a la prestación de servicios de TI sobre la seguridad.

- **Falta de autonomía:** puede limitar la autonomía del CISO y su capacidad para actuar de forma independiente. Si el CIO no apoya la función de seguridad o no proporciona recursos suficientes, el CISO puede tener dificultades para implementar controles de seguridad de forma eficaz.

- **Barreras de comunicación:** pueden limitar su capacidad de comunicación con el CEO y el Consejo de Administración para comprender la postura de seguridad de la organización.

- **Escasa atención a la seguridad:** puede reforzar la percepción de que la seguridad es una preocupación secundaria y no recibir la atención y los recursos que merece.

- **Cumplimiento frente a gestión de riesgos:** el hecho de que el CIO se centre en la prestación de servicios de TI puede conducir a veces a un enfoque de la seguridad centrado en el cumplimiento, en el que se hace hincapié en cumplir los requisitos normativos en lugar de gestionar los riesgos de seguridad.

En general, aunque el hecho de que el CISO dependa del CIO puede ser beneficioso, es importante abordar estos posibles problemas para garantizar que se preste a la seguridad la atención que merece y que el CISO puede operar de forma independiente y proporcionar una evaluación objetiva de la postura de seguridad de la organización.

¿Qué hacer a partir de ahora?

Es crucial que la ciberseguridad se alinee con los objetivos empresariales, porque los riesgos pueden afectar directamente a la capacidad de una empresa para alcanzar sus objetivos estratégicos. Cuanto mejor alineada esté la ciberseguridad con la empresa, más resistente será ésta Y más podrá prosperar.

Pasar del «yo» al «nosotros»

La creación de una alineación eficaz entre seguridad y empresa requiere una combinación de habilidades. Exige métricas compartidas. Pero, sobre todo, requiere una aplicación amplia y coherente en toda la organización. Los responsables de ciberseguridad deben colaborar estrechamente con otras funciones para asignar los recursos adecuados y tomar decisiones.

Además, a medida que las organizaciones escalen la montaña «del yo al nosotros», tendrán que pensar de forma muy diferente sobre cómo ven el propósito de la ciberseguridad. En lugar de considerar la responsabilidad del equipo de ciberseguridad puramente en términos de protección de recursos, deben ampliar su perspectiva para incluir objetivos empresariales estratégicos. Esa perspectiva debe plasmarse en cada evaluación, en cada informe al Consejo de Administración y en cada comunicación que el equipo de seguridad comparta con el resto de la organización.

Solo entonces podrán las organizaciones garantizar la ciberresiliencia y lograr un crecimiento empresarial sostenible.

Metodología

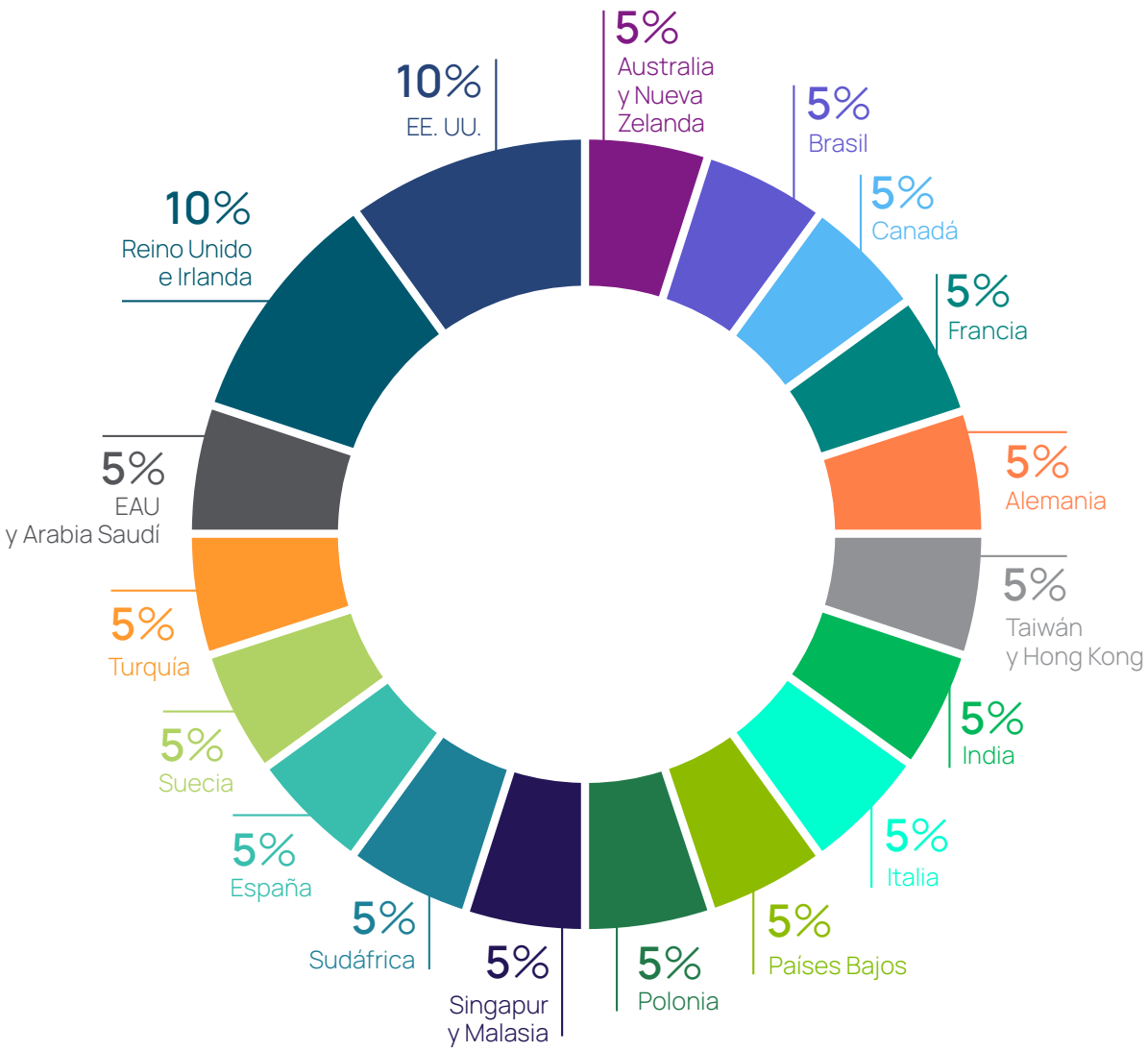
La encuesta recogió respuestas de 2007 personas durante el mes de marzo de 2023.

Incluye respuestas de los directivos, la dirección de los departamentos y los niveles de gestión de las organizaciones. Los encuestados proceden de 23 países y 22 sectores, y trabajaban en empresas con 500 empleados o más.

Todos los participantes afirmaron haber tomado parte en la toma de decisiones en materia de seguridad como responsables últimos, como parte de un equipo o como personas influyentes.

Los resultados no están ponderados.

País: ¿En qué país vives?

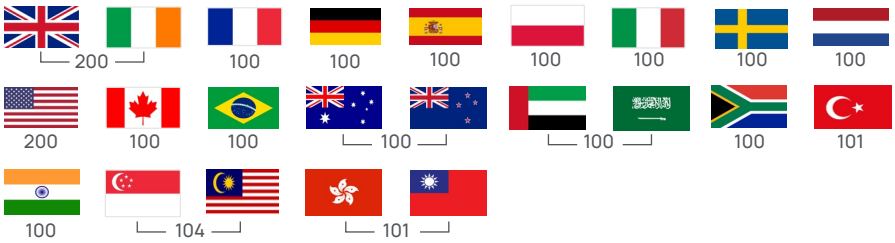


Resumen demográfico de los encuestados

Datos demográficos

Total de encuestados: **2007**

País de residencia



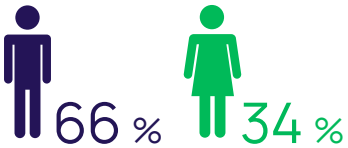
Tipo de función

Tamaño de la empresa

N.º de empleados	500-999	1000-4999	5000+
% de encuestados	35 %	40 %	26 %

Sector de actividad

Sexo y edad

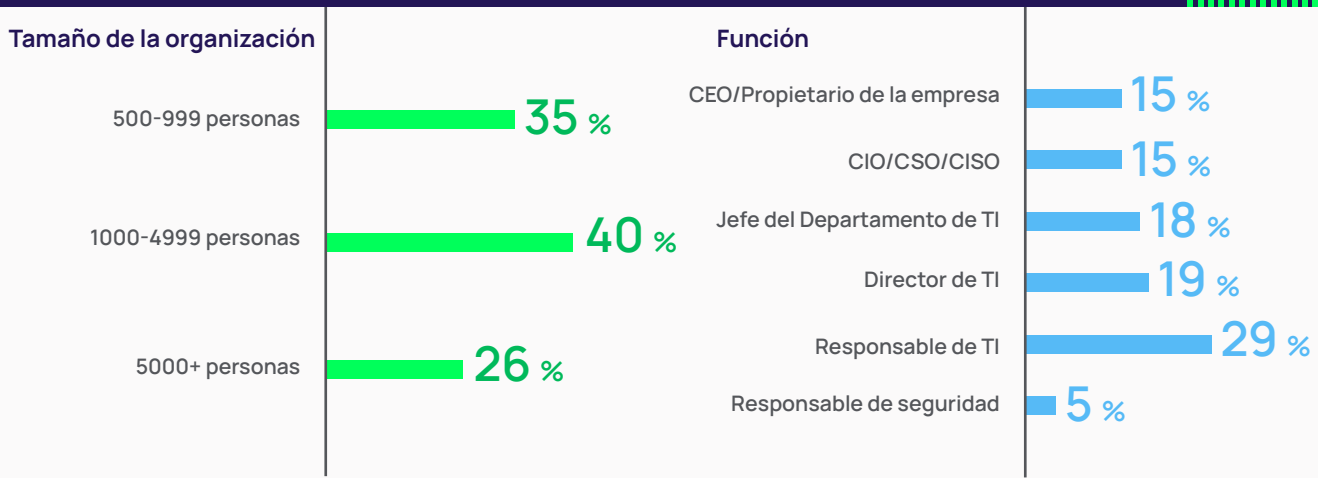


El 66% de los encuestados eran hombres y el 34 % mujeres

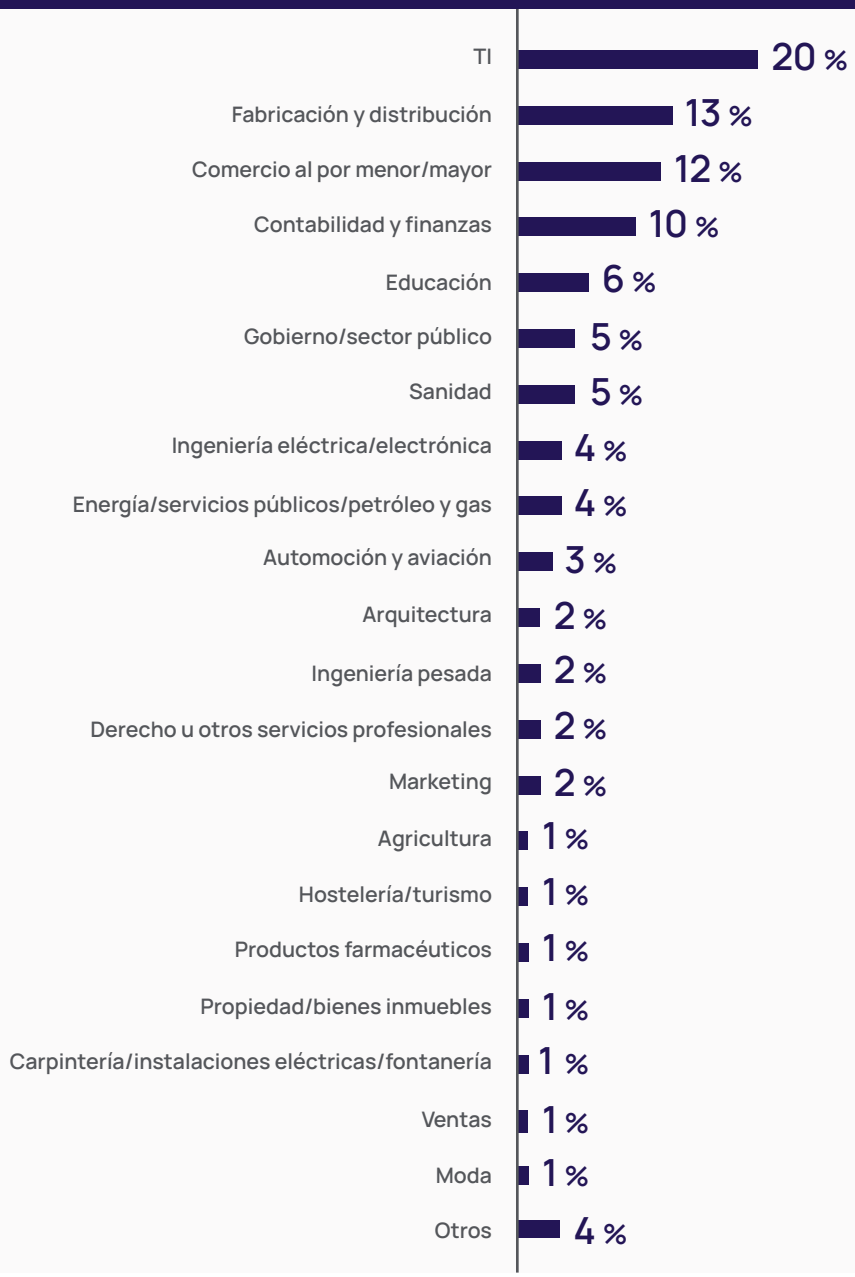
de los encuestados tenían entre

25-44

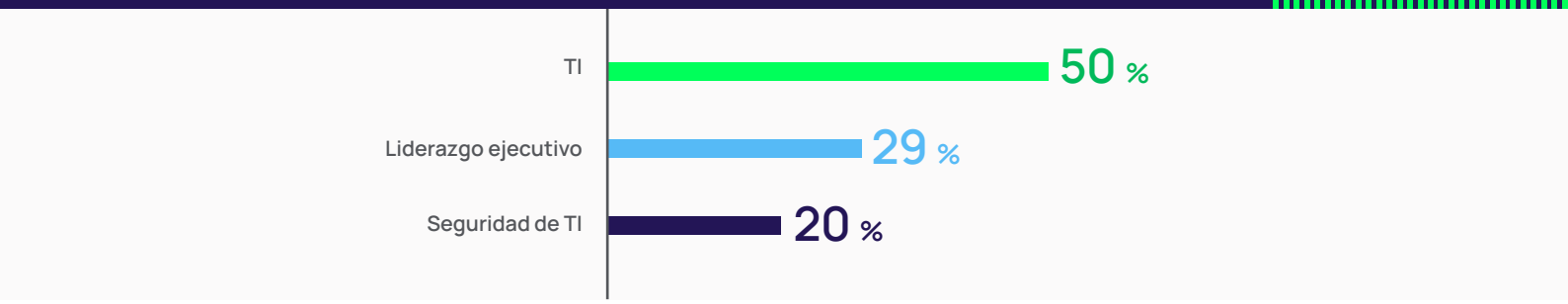
Tamaño de la organización y función: ¿Cuántas personas emplea la organización para la que trabajas? ¿Cuál de las siguientes opciones describe mejor tu función?



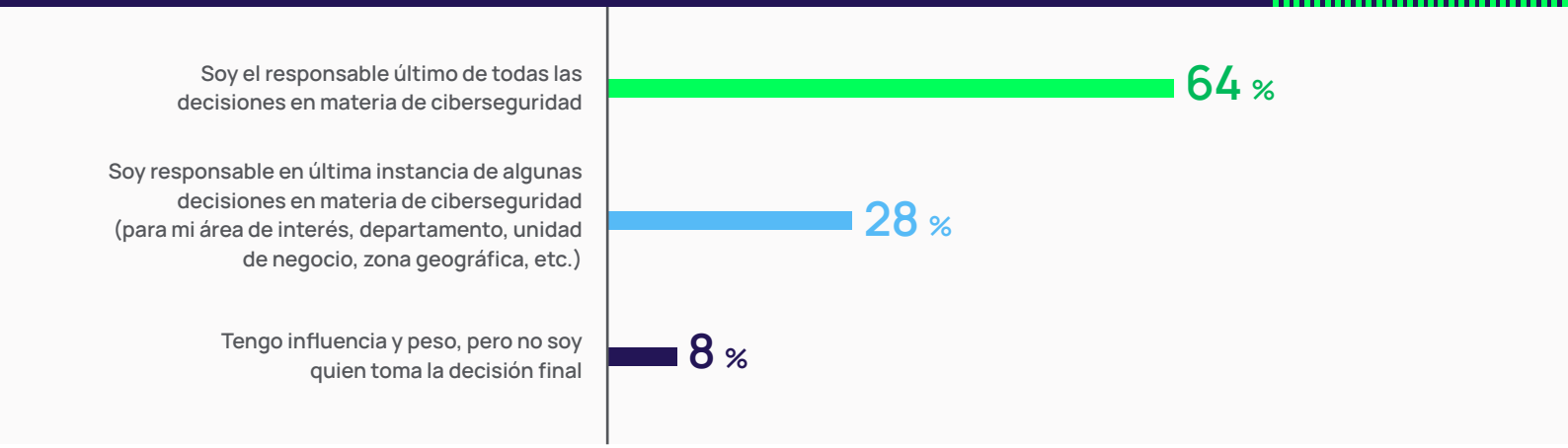
Sector: ¿Cuál de estas opciones describe mejor tu sector industrial?



Departamentos: ¿En cuál de los siguientes departamentos trabajas?



Responsabilidad: ¿ En qué medida eres responsable de la toma de decisiones en materia de ciberseguridad en tu organización?



Delinea

Securing identities at every interaction

Delinea es pionera en la protección de identidades a través de la autorización centralizada, haciendo que las organizaciones actuales sean más seguras al gobernar sin problemas sus interacciones en entornos complejos. Delinea permite a las organizaciones aplicar el contexto y la inteligencia en todo el ciclo de vida de la identidad a través de la nube y la infraestructura tradicional, los datos y las aplicaciones SaaS para eliminar las amenazas relacionadas con la identidad. Con la autorización inteligente, Delinea proporciona la única plataforma que permite descubrir todas las identidades, asignar niveles de acceso adecuados, detectar irregularidades y responder inmediatamente a las amenazas de identidad en tiempo real. Delinea acelera la adopción por parte de sus equipos al desplegarse en semanas, no en meses, y los hace más productivos al requerir un 90% menos de recursos para su gestión que el competidor más cercano. Con un tiempo de actividad garantizado del 99,99%, Delinea Platform es la solución de seguridad de identidad más fiable disponible. Obtenga más información sobre Delinea.com, **LinkedIn**, **X**, y **YouTube**.